Retail Energy Supply Association

April 29, 2019

**VIA ELECTRONIC MAIL**

Hon. Kathleen H. Burgess
Secretary of the Commission
New York State Public Service Commission
Three Empire State Plaza
Albany, New York 12223-1350

**RE: Case 18-M-0376 - Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place**

**Case 18-M-0084 - In the Matter of a Comprehensive Energy Efficiency Initiative**

**Case 16-M-0411 - In the Matter of Distributed System Implementation Plans**

**Case 15-M-0180 - In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products**

**Submission of Response to the Petition of the Joint Utilities for Declaratory Ruling**

Dear Secretary Burgess:

On behalf of the Retail Energy Supply Association ("RESA"), attached for filing please find RESA's Response to the Petition of the Joint Utilities for approval of the business-to-business process used to formulate a data security agreement and for affirming the joint utilities' authority to require and enforce execution of the data security agreement by entities seeking access to utility customer data or utility systems.

We greatly appreciate your attention to this matter. If the Commission has any questions or comments regarding this request, please do not hesitate to contact the undersigned.

Respectfully Submitted,

**/s/ Tracy McCormick**
Tracy McCormick

Executive Director of the Retail Energy Supply Association

Post Office Box 6089 Harrisburg, Pennsylvania 17112 www.resausa.org
tmccormick@resausa.org 717-566-5405

**STATE OF NEW YORK**
**PUBLIC SERVICE COMMISSION**

| | |
|---|---|
| **Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place.** | **Case 18-M-0376** |
| **In the Matter of a Comprehensive Energy Efficiency Initiative.** | **Case 18-M-0084** |
| **In the Matter of Distributed System Implementation Plans.** | **Case 16-M-0411** |
| **In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products.** | **Case 15-M-0180** |

# RETAIL ENERGY SUPPLY ASSOCIATION'S RESPONSE TO THE PETITION OF THE JOINT UTILITIES FOR APPROVAL OF THE BUSINESS-TO-BUSINESS PROCESS USED TO FORMULATE A DATA SECURITY AGREEMENT AND FOR AFFIRMING THE JOINT UTILITIES' AUTHORITY TO REQUIRE AND ENFORCE EXECUTION OF THE DATA SECURITY AGREEMENT BY ENTITIES SEEKING ACCESS TO UTILITY CUSTOMER DATA OR UTILITY SYSTEMS

**Dated: April 29, 2019**

## PRELIMINARY STATEMENT

The Retail Energy Supply Association ("RESA" or "Association")[1] respectfully submits this Response to the *Joint Utilities' Petition for Approval of the Business-to-Business Process Used to Formulate a Data Security Agreement ("DSA") and for Affirming the Joint Utilities' Authority to Require and Enforce Execution of the Data Security Agreement By Entities Seeking Access to Utility Customer Data or Utility Systems* ("Petition") that was filed on February 4, 2019 with the New York State Public Service Commission ("Commission").[2] RESA hereby submits this Response pursuant to the *Notice Soliciting Comments* issued on February 20, 2019 in the above-captioned proceedings ("Notice").

As a threshold matter, RESA and its members recognize the need for robust data security protocols to protect sensitive and confidential consumer information. All energy market participants have an interest in protecting the integrity of the networks that deliver energy services to millions of New Yorkers, and achieving optimal cyber protocols which sufficiently engage the necessary protections. Importantly, however, such protections should not be overly burdensome or duplicative, and standardization of cyber security protocols should not be

---

1 This filing represents the positions of the Retail Energy Supply Association as an organization, and may not represent the views of any particular member of the Association. Founded in 1990, RESA is a broad and diverse group of twenty retail energy suppliers dedicated to promoting efficient, sustainable and customer-oriented competitive retail energy markets. RESA members operate throughout the United States delivering value-added electricity and natural gas service at retail to residential, commercial and industrial energy customers. More information on RESA can be found at www.resausa.org.

2 Case 18-M-0376, *et al.*, Joint Utilities' Petition for Approval of the Business-to-Business Process Used to Formulate a Data Security Agreement and for Affirming the Joint Utilities' Authority to Require and Enforce Execution of the Data Security Agreement By Entities Seeking Access to Utility Customer Data or Utility Systems (February 4, 2019) (hereinafter "Petition").

achieved at the expense of tailored solutions that address the unique aspects of each stakeholder's role in the marketplace.

RESA was an active participant in the initial business-to-business process described below and was engaged to further the overarching objective of this matter – achieve optimal cyber protocols that incorporate necessary/reasonable industry-recognized protections without enacting barriers to market participation and onerous cyber requirements. RESA remains committed to ensuring customer data is appropriately protected.

In its Petition, the Utilities[3] ask the Commission for relief on three issues: "(1) approve the continuing business-to-business process to develop and implement a DSA to protect customer information and utility IT systems; (2) approve minimum standard requirements in the DSA subject to the continuing evolution of the DSA; and (3) affirm the Joint Utilities' existing authority to require ESEs to submit and execute a DSA and, if they fail to do so, disconnect them from the utility's IT systems and remove their access to customer information in order to protect customers and utilities from a potential cyber security event."[4]

Procedurally, and as described more fully below, the Utilities' requested relief had been previously set forth by the Utilities in various other petitions to the Commission that are still pending. The Commission's Notice sets forth the three additional related petitions that it is simultaneously considering regarding cyber security and the DSA. Given that the Utilities

---

[3] As used herein, the term "Utilities" means and includes Consolidated Edison Company of New York, Inc., Orange and Rockland Utilities, Inc., Central Hudson Gas & Electric Corporation, National Fuel Gas Distribution Corporation, The Brooklyn Union Gas Company d/b/a National Grid NY, KeySpan Gas East Corporation d/b/a National Grid, Niagara Mohawk Power Corporation d/b/a National Grid, New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation.

[4] Petition at 17.

have not withdrawn such other requests for relief, RESA incorporates herein its prior responses to pending matters related to the DSA and cyber security.

RESA urges the Commission to reject the instant Petition. First, the Utilities are requesting an improper delegation of authority that, if granted, would create a dangerous precedent for future matters. Second, the "living" business-to-business approach requested by the Utilities is inequitable and does not result in balanced outcomes due to the imbalance of power between the parties. Third, the Utilities ask the Commission to approve contract provisions that were never proposed as part of a formal rulemaking process.

## BACKGROUND

The Utilities initially sought to require ESCOs doing business on their systems to execute Data Security Agreements ("DSA") and Vendor Risk Assessments ("VRA") following a cyber security incident in the spring of 2018. On May 31, 2018, Department of Public Service Staff ("Staff") facilitated a meeting with the Utilities, ESCOs and ESCO representatives, and electronic data interchange ("EDI") providers, for the Utilities to explain their reasoning for imposing the new requirements. The ESCOs voiced their initial concerns about the DSA framework and utility-proposed "business-to-business" process during that meeting.

On June 14, 2018, following ESCO industry requests for the formal docketing and initiation of an associated regulatory process with respect to the development of DSAs and VRAs, the Commission commenced Case 18-M-0376 to address cybersecurity protection in the energy marketplace. In its Order instituting that proceeding, the Commission directed involved parties (including the Utilities and ESCOs) to engage in a "business-to-business" process to address cyber security issues, and for Staff to review the process and submit a report thereon to the Commission. Thereafter, the Utilities and ESCOs engaged through an in-person meeting,

multiple conference calls, and the exchange of comments and drafts of the DSA, and the successor to the VRA – the Self-Attestation document ("SA").

While the business-to-business process provided a forum for cyber security issues to be discussed between the parties, it did not result in universal agreement, nor were ESCO concerns about the non-mutual nature of the draft DSA and SA adequately addressed. Many ESCOs took issue with the fact that the DSA provided the Utilities with significant authority over ESCO operations (including but not limited to audit rights, restrictions on derivative data uses in a manner that could undermine product development, restrictions on locations for ESCO processing and information storage, and a new and overly burdensome $5 million cyber-insurance requirement). The Utilities made few concessions to the ESCOs during the business-to-business process, resulting in a DSA and SA that were skewed heavily in the Utilities' favor, and shifted an unreasonable amount of cyber security risk and liability onto the ESCOs.

While this business-to-business process still was ongoing, and with much substantive disagreement still existing between the parties over the terms of the DSA, on August 16, 2018, the Utilities circulated an e-mail pronouncing:

> "The Joint Utilities consider the DSA, and the previously sent Self-Attestation, to be final. ESEs must submit the completed and signed Self Attestation by August 24, 2018. Modified Self Attestation are not acceptable. As previously stated comments explaining the status of compliance for each question are encouraged so that the Utilities can work with the ESEs to attain adequate security at this time. If you have already submitted an executed non-modified Self Attestation, you do not need to submit the final Self Attestation. If you submitted a modified or unexecuted Self Attestation, you must submit and execute the final Self Attestation. The final DSA must be executed and submitted to the applicable Utilities by August 31, 2018."

Given this short deadline, many ESCOs submitted signed DSAs under protest, while other ESCOs did not submit a signed DSA to the Utilities at all. Thereafter, on September

24, 2018, Staff filed its "Report on the Status of the Business-to-Business Collaborative to Address Cyber Security in the Retail Access Industry" ("Staff Report"), which concluded that the business-to-business process "resulted in a balanced DSA" despite the fact that many ESCO concerns about the DSA and SA remained unaddressed. Also missing was any affirmation from the market also agreeing that the DSA was a balanced compromise.

On November 9, 2018, the Utilities filed a Petition ("November 2018 Petition") seeking a declaratory ruling from that the Commission that they had the right, under the UBP, to unilaterally discontinue ESCO access to utility systems for those ESCOs that failed to sign and return a DSA. Notably, in the November 2018 Petition, the Utilities expressed their unfounded position that "the UBPs permit individual utilities to initiate the discontinuance process pursuant to UBP Section (2)(F)(2) without intervention of the Commission." RESA and many other parties submitted Comments challenging the November 2018 Petition, *inter alia*, on the grounds that: allowing such an outcome would effectively constitute an amendment of the UBP without having adhered to the rulemaking requirements of the State Administrative Procedure Act ("SAPA"); and allowing unilateral utility discontinuance of ESCO access without Commission intervention violated the UBP; and accepting the business-to-business process as an appropriate method for the Utilities to implement (and, in the future, amend) the DSA would set a dangerous precedent in both New York and in other states.[5] The November 2018 Petition currently is pending before the Commission.

[5] *See* Case 18-M-0376 *et al.*, supra, Retail Energy Supply Association's Response to the Petition of the Joint Utilities for Declaratory Ruling Regarding their Authority to Discontinue Utility Access to Energy Service Companies in Violation of the Uniform Business Practices (filed December 21, 2018).

Separately, on November 30, 2018, Mission:data Coalition, Inc. ("Mission:data") filed a Petition for a Declaratory Ruling seeking to exempt DERS from the Utilities' cyber security requirements ("Mission:data Petition").[6] Specifically, Mission:data argued that there is no Commission requirement that DERS must sign a DSA or an SA in order to utilize Green Button Connect ("GBC") as offered by the Utilities. The Mission:data Petition also currently is pending before the Commission.

On December 13, 2018, the Commission issued an Order in its energy efficiency proceeding, Case 18-M-0084. In the Energy Efficiency Order, the Commission, *inter alia*, directed the Utilities and Staff to conduct a collaborative with DER providers and other stakeholders to develop appropriate Terms and Conditions for third parties to access data through Green Button Connect ("GBC") and more comprehensively examine data access.[7] The Commission specifically referenced the business-to-business process that had resulted in the controversial ESCO DSA,[8] and stated that "in the event the collaborative does not produce a mutually agreed upon agreement, Staff will propose GBC terms and conditions based on successful terms utilized in other jurisdictions."[9] Several GBC working group meetings have since occurred.

---

6 Case 18-M-0376, supra, Petition of Mission:data Coalition for Declaratory Ruling Regarding the DER Oversight Order's Exemption of DER Suppliers from Certain Cybersecurity Requirements (filed November 30, 2018).

7 Case 18-M-0084, In the Matter of a Comprehensive Energy Efficiency Initiative, Order Adopting Accelerated Energy Efficiency Targets (issued December 31, 2018), p. 44 ("Energy Efficiency Order").

8 *Id.* at n. 58 (clearly acknowledging that "parties disagree on numerous aspects of the current DSA").

9 *Id.* at 44-45.

Notwithstanding the Commission's December Energy Efficiency Order that provided for a forthcoming collaborative to address data access, the Utilities filed the instant Petition on February 7, 2019 requesting that the Commission, once and for all, confirm that the business-to-business process used by the Utilities to arrive at the current iteration of the DSA and SA, was appropriate, and that such process be utilized going forward to develop or amend the DSA. Importantly, in the Petition, the Utilities request the Commission's blessing not only of its actions to develop the DSA for ESCOs, but that the business-to-business process be applicable to all ESCOs, DERS, Direct Customers, and their applicable contractors (collectively, "Energy Service Entities" or "ESEs"). Finally, the Utilities seek Commission confirmation that they have the authority to prohibit any ESE (ESCOs or otherwise) from accessing utility systems or customer data if such ESE has not satisfactorily completed the Utility-developed DSA, without Commission intervention.

## ARGUMENT

## POINT I

### THE PETITION SHOULD BE REJECTED BECAUSE THE UTILITIES SEEK AN IMPROPER DELEGATION OF AUTHORITY

The Petition asks the Commission to affirm the Utilities' right to impose the DSA on ESEs, and "disconnect them from the utility's IT systems and remove their access to customer information in order to protect customers and utilities from a potential cyber security event" without Commission intervention.[10] The Utilities seek a delegation of authority that should

[10] *See* Petition Attachment 2, pp. 7-8.

remain with the Commission. Providing such authority to the utilities introduces a dangerous precedent for future matters.

1. Commission Intervention is Required Pursuant to the UBP

Neither the UBP nor the Utilities' tariffs (which are reviewed and approved by the Commission and subject to Commission oversight) provide the Utilities with the authority to discontinue ESCO interactions without Commission intervention. Specifically, Section 2 of the UBP provides that Commission oversight is to be present when initiating a discontinuance. Importantly, a discontinuance requires a case-specific finding under Section 2.F.1 that there is *cause* to discontinue an ESCO.

Moreover, UBP Sections 2.F.4 and 2.F.5 explicitly provide that the Commission is to play an active role in a discontinuance process, and that the utility seeking to discontinue service "shall submit a sample copy of its discontinuance notice to the Department for review and approval prior to distribution to customers." Section 2.F.5 provides that a utility "may request permission from the Department to expedite the discontinuance process upon a showing that it is necessary for safe and adequate service or in the public interest."

On its face, the UBP unequivocally calls for Commission intervention before a utility may discontinue ESCO service. This is because the Commission is the only entity able to weigh all of the pertinent factors objectively in rendering a decision. The UBP was developed to provide ESCOs with basic due process rights. If the Utility is seeking an amendment to the UBP, this would need to be done by the Commission pursuant to the rules of SAPA, as only the Commission has rulemaking authority for the retail markets. RESA discussed the application of

SAPA in its December 21, 2018 *Response to the Petition of the Joint Utilities for Declaratory Ruling* and such arguments are incorporated herein and attached hereto as Attachment 1.[11]

As a matter of policy, transferring enforcement of Commission rules and policies to the Utilities runs contrary to Commission precedent. To provide the Utilities with unchecked power to interpret and implement Commission rules and policies could also have the consequence of hindering competitive markets – both retail supply and DER – because the ESEs and the Utilities are often in direct competition. As previously noted by RESA, checks and balances are a fundamental part of agency regulation and granting the Utilities' request to be the judge and enforcement arm of a dispute to which it is also a party, with no Commission oversight, runs contrary to logic. Providing the Utilities with such unilateral power has the potential to stymie the Commission's REV and clean energy initiatives.

2. Failure to Execute a DSA Does Not Trigger the Discontinuance Process in the UBP

As a threshold matter, the UBP provision cited to by the Utilities as granting the Utilities the authority to require ESCOs to execute the DSA is flawed. The Utilities rely on UBP Section 2: Eligibility Requirements (F).1.a which provides that:

> Failure to act that is likely to cause, or has caused, a significant risk or condition that compromises the safety, system security, or operational reliability of the distribution utility's system, and the ESCO or Direct Customer failed to eliminate immediately the risk or condition upon verified receipt of a non-EDI notice.

[11] *See* Case 18-M-0376 *et al.*, supra, Retail Energy Supply Association's Response to the Petition of the Joint Utilities For Declaratory Ruling Regarding Their Authority to Discontinue Utilities Access to Energy Service Companies in Violation of the Uniform Business Practices (filed December 21, 2018).

First, the Utilities have failed to provide evidence of risk associated with ESCOs operating pursuant to the status quo absent a DSA. The reports titled *Cost of Compliance With Data Protection Regulations* and *2017 Cost of Cyber Crime Study* included as Petition Attachments 7 and 8, respectively, are red herrings, and do not identify a direct causal relationship between actual risk and ESCO execution of a DSA. Moreover, the reports relied upon in the Petition are not tailored to the energy industry or utility interaction with ESCOs and have zero probative value to the Commission's review.

Second, the DSA is nothing more than a contractual agreement governing liability and does not actually ensure that the utility network is not compromised by EDI transactions. The DSA itself does not increase or decrease any perceived risk to a utility's system, nor does executing the agreement mitigate any such perceived risk. As the Utilities note, "The Joint Utilities face the constant risk of cyber-attacks and consequently, maintain cyber security defenses. If these defenses fail, the utility could suffer a cyber security incident and its effects, including significant costs, and regulatory and reputational issues."[12] If, assuming *arguendo*, the above-mentioned UBP provision was intended to capture cyber security risk (which RESA argues it does not), there is a complete lack of evidence from the Utilities demonstrating that ESCOs pose a risk absent a DSA and a DSA remedies such risk. Instead, the Utilities are attempting here to impose customer privacy regulations on ESCOs through a DSA, when such regulations should be determined through a proper rulemaking process where unintended consequences can be minimized through a larger stakeholder lens. Had the DSA been developed through a rulemaking, issues ESCOs are currently seeing, such as adverse reactions from

[12] Petition at 4-5.

customers and other parties who receive encrypted messages from their suppliers could have been anticipated and avoided.

Assuming, *arguendo*, that the above-noted UBP provision does stand for the proposition by which the Utilities assert (which RESA contests), as discussed *supra*, there is a due process component that requires Commission intervention and determination on a case by case basis. For these reasons, the Commission must continue to exercise close jurisdiction to over its policies and initiatives.

## POINT II

## THE PETITION SHOULD BE REJECTED BECAUSE THE REQUESTED BUSINESS-TO-BUSINESS APPROACH IS INEQUITABLE

In the Petition, the Utilities seek Commission confirmation that the business-to-business process used in this case was appropriate for the development of the DSA, that it continue to be used in the future as DSA amendments are needed, and that it be applicable to all ESEs (not only ESCOs). For the reasons set forth below, the Commission should not retroactively approve the business-to-business approach as appropriate for past development of the DSA, and should reject its continued use going forward, in favor of a more formal process that equally weighs the input from market participants and data protection industry experts.

RESA recognizes the need for robust cyber security protocols in today's technology-dependent landscape, and is not opposed to the development and implementation of reasonable cybersecurity standards for ESEs through a fair and equitable process. Throughout the course of these proceedings, however, it has become clear that the business-to-business process endorsed by the Utilities is neither fair nor equitable. Instead, it eliminates the need for Commission oversight over the contents of the DSA, and provides the Utilities with unfettered discretion to unilaterally impose cyber security requirements on ESEs as and when they see fit.

As noted above, the current form of the DSA, *inter alia*, would grant the Utilities audit rights over ESCO operations, restrict derivative data uses in a manner that could undermine DER product development, restrict locations for ESCO processing and information storage, and impose a new (and overly burdensome) $5 million cyber-insurance requirement.[13] These onerous requirements were opposed by many ESCOs, but refusal by the Utilities during business-to-business "discussions" with stakeholders to compromise on provisions allowed many aspects of the DSA to remain without much modification, despite ESCO disagreement.

Later, despite many stakeholder-voiced concerns about how these provisions shifted an unreasonable amount of risk onto the ESCOs and were overly imbalanced in favor of the Utilities, the Utilities nonetheless declared the DSA to be "final" and demanded that ESCOs sign and return it to the Utilities. This ability to unilaterally determine the finality of an important document, or to impose additional conditions of service upon ESCOs in the future, without addressing legitimate concerns raised by market participants (who are competitors of the Utilities), only demonstrates the inequity of the business-to-business process used, and that if the Commission bestows the Utilities with such unbridled power, it would significantly harm the energy marketplace.

To be clear, RESA does not oppose the use of a collaborative process between the Utilities, stakeholders, and security experts to better understand whether, and to what extent, revisions to the DSA are needed. Open dialogue between parties can help them address issues related to cyber security, particularly as they evolve over time, and revise the DSA as necessary to accommodate future circumstances. However, the process used by the Utilities here fell short

[13] *See* Case 18-M-0376, supra, *et al.*, Petition for Commission Guidance and Related Request for Modification to the Procedural Schedule of the National Energy Marketers Association (filed August 21, 2018), pp. 7-11.

of, and hardly resembles, any stakeholder collaborative process that have been deployed in the past by the Commission.

In a standard collaborative process, stakeholders engage in discussions to develop a solution to a problem, which then is reported to the Commission, subjected to a formal comment period under SAPA, and finally acted upon by the Commission through an order. Those crucial steps are missing here. Instead, the business-to-business process that has been exercised thus far has not required any Commission approval of the DSA (or potential future amendments thereto). Rather, the Utilities are free to determine what they believe are the appropriate DSA requirements, and enforce those requirements with unlimited discretion.

Without Commission oversight, future changes to the DSA while couched in the guise of a "collaborative" process, may in reality be a one-sided discussion with the Utilities determining the outcome, as already demonstrated by the myriad of DSA concerns enumerated by the ESCO community that were wholly ignored. RESA urges the Commission to put an end to this informal business-to-business process and instead exert oversight over its policies, including data security. Development of a DSA, or of cyber security protocols as a condition to ESCO/DERS eligibility, should be accomplished through standard rulemaking procedures.

The Utilities repeatedly cite to the Staff Report's finding that "the business-to-business process has enabled a productive dialogue and has resulted in a balanced DSA" to justify their determination that the DSA (and the process through which it was "developed") is acceptable, and that it is appropriate to demand that ESCOs comply with it or face a discontinuation of ESCO service.[14] RESA notes, however, that the Staff Report was issued over

[14] Staff Report at 8. As already noted above, the UBP does not authorize the Utilities to unilaterally discontinue ESCO service without Commission intervention.

a month *after* the Utilities already had declared the finality of the DSA and SA. In other words, the Staff Report has no bearing on the Utilities' decision to impose the DSA. This further demonstrates the power that would be wielded by the Utilities if the Commission allows the Utilities to continue utilizing the business-to-business process to regulate data security matters.

Based on the foregoing, RESA respectfully urges the Commission to find that the business-to-business process without Commission involvement has been an inappropriate means of developing the DSA. Instead, the Utilities should be required to adhere to standard rulemaking procedures, and seek Commission approval of any DSA and SA (or future amendments thereto), subject to a full stakeholder comment process. For example, if the Commission determines that the requirements of the DSA actually represent conditions of ESCO or DERS service, then the appropriate procedure would be for each utility to file proposed tariff amendments incorporating such conditions, and allow stakeholders an opportunity to comment thereon.

If a collaborative process is preferable, then the Commission should ensure that such collaborative process affords stakeholders adequate opportunity to participate in and shape discussions about data security, and that the Utilities do not have unchecked power to impose their policies on the retail markets under the guise of cooperation. Such collaborative also should adhere to standard SAPA procedures, *i.e.*, any DSA resulting from such process be filed for Commission approval, and also be subject to a formal notice and comment period.

## POINT III

## THE UTILITIES' REQUEST FOR COMMISSION APPROVAL OF THE DSA PROVISIONS SHOULD BE REJECTED

The Petition requests Commission approval of the provisions included in the DSA itself. RESA, along with a number of other parties, engaged with the Utilities to discuss the DSA at length. RESA offered numerous suggested revisions to the DSA, and attempted to negotiate such provisions with the Utilities over several meetings. Some of the significant concerns with the DSA that were never sufficiently resolved include: (i) determining what constitutes "Confidential Utility Information"; (ii) establishing a cause/effect and limitation of liability with respect to inclusion of any indemnification provision; and (iii) revising the DSA to include mutual data protections for the Utilities and ESCOs.

In the interest of brevity, RESA will not restate its analysis regarding the deficiencies of the DSA provisions. Instead, attached to this Petition Response as Attachment 2 are RESA's *Comments On Proposed Data Security Agreement* that were filed in with the Utilities on July 2, 2018.

## CONCLUSION

For the foregoing reasons, RESA respectfully requests that the Commission deny the Utilities' Petition.

Respectfully Submitted,

**/s/ Tracy McCormick**
Tracy McCormick

Executive Director of the Retail Energy Supply Association